A CERTIFICATELESS SIGNATURE SCHEME WITHOUT RANDOM ORACLES

Trinh Viet Cuong

Received: 15 March 2017 / Accepted: 7 June 2017 / Published: July 2017

Abstract: *In the context of certificateless public key cryptography, there is no need to use the certificate to certify the public key, and neither the user nor the authority can derive the full private key by himself. There have been several efforts to propose a certificateless signature (CLS) scheme in the standard model, but all of them either make use of the Waters' technique or of the generic conversion technique which both lead to inefficient schemes. In this paper, we introduce a new and direct approach to construct a CLS scheme, secured in the standard model, with constant-size of all parameters and having efficient computing time. Our scheme is therefore very efficient when comparing to existing CLS schemes in the standard model.*

Keywords: *Certificateless, signature, standard model, strong adversary.*

1. Introduction

The era of modern cryptography has started with the introduction of public key cryptography (PKC). In the context of PKC, each user possesses a private key (e.g., to digitally sign a message) and a corresponding public key (e.g., to verify the obtained signature). To verify whether a public key belongs to the correct identified user, the public key needs to be associated to a certificate provided by a trusted Certificate Authority (CA), introducing the notion of Public Key Infrastructure (PKI). During the life-cycle of e.g., a signature scheme, the PKI is therefore in charge of providing, maintaining and revoking a large amount of certificates, which requires using a lot of resources when deployed in the real world. To deal with this drawback, Shamir [13] has introduced the concept of identity-based cryptography for which the public key of a user is exactly his/her identity, such as his/her phone number or email address. The corresponding private key is next generated by some private key generator (PKG), from a master secret key and the identity of the requesting user. However, identity-based cryptography naturally suffers an important disadvantage (named key escrow problem): the PKG knows the private key of all users. One basic solution is to distribute the key of the PKG into several entities. But first, such distribution is not compatible with all identity-based schemes, or leads to non-efficient solutions. And second, the whole infrastructure may become too complex for a practical deployment.

Trinh Viet Cuong
Faculty of Information and Communication Technologies, Hong Duc University
Email: Trinhvietcuong@hdu.edu.vn (✉)

Certificateless Cryptography. To eliminate this new problem, Al-Riyami and Paterson have introduced in [1] the notion certificateless cryptography. There is still no need for a certificate and, this time, the PKG has no way to obtain the user private key. In fact, the key is computed by both the PKG and the user such that only the latter obtains the result. The part which is still provided by the PKG is computed from a master secret key and the user's identity.

We now focus on the case of certificateless signature (CLS) schemes and give some words about related work before explaining our contribution on this topic.

1.1. Related work on certificateless signature schemes

To date, there have been numerous efforts to propose CLS schemes in both the random oracle (using hash function in the construction and then model it as random oracle in the security proof) [1], [9], [21], [4], [14], [16], [8] and the standard models (not model hash function as random oracle in the security proof) [20], [7], [10], [17], [19], [18]. Al-Riyami and Paterson [1] have proposed the first CLS scheme, but Huang et al. [9] have then pointed out that their work is insecure.

Regarding constructions secure on the random oracle model, Zhang et al. [21], Choi et al. [4], and Tso et al. [14] have proposed three efficient CLS schemes, where all parameters are of constant-size. In [8], Huang et al. go one step further by revisiting the security model and proposing two efficient constructions in the random oracle model.

We now focus on the constructions that are secure in the standard model. In this case, there are currently two types of constructions in the literature.

Using Waters' hash function. In [15], Waters has proposed a new hash function technique that can be used to map an identity (of arbitrary length) to a key (of fixed bit length) in a CLS scheme. The main problem of such technique is that it leads to relatively large public parameters and heavy computing time. More precisely, both the space and time complexities are a function of the size of the expected fixed bit length. One possibility is then to apply the Naccache's [11] or Chatterjee-Sarkar's [3] techniques to reduce this fixed length, but the price to pay is either a security loss or a less efficient scheme.

The first concrete construction using Waters' hash function has been given by Liu et al [10]. Three other schemes can now be found in the literature [17], [19], [18].

Yum-Lee generic transformation. In [20], Yum and Lee have introduced a generic construction for certificateless signature schemes (applied in both the random oracle and the standard models). The first step of this construction consists in designing an identity-based signature (IBS) scheme and then combining it with a standard signature (SS). The resulting efficiency for the CLS scheme is however approximately worse than the one of the chosen IBS plus the one of the chosen SS. Moreover, a way to construct an IBS scheme is to apply the folklore conversion technique which either uses two SS schemes or a 2-level Hierarchical Identity-Based Encryption (but we then fall into the above case of using Waters' technique). Again, the resulting efficiency is approximately three times worse than the efficiency of the underlying SS scheme. It is also worth to remark that Hu et al. [7] have pointed out that Yum

and Lee's technique is insecure against a Type I forger. They have next given a modification but at the price of a loss in terms of efficiency.

To the best of our knowledge, it then remains an open problem to design a truly efficient CLS scheme secure in the standard model. In this paper, we propose such construction by providing a new technique.

1.2. Our contribution and organization of the paper

Our construction is based on the stacking of the Boneh-Boyen BB standard signature [2] in the recent Pointcheval-Sanders PS one [12], both secure in the standard model. More precisely, the generator used in the PS signature corresponds to a BB signature including the master secret key and user's identity. Adding one element in the signature, we obtain a unique pairing equation to verify both the validity of our CLS and the one of the related public key, instead of two if basically applied together, or if other standard signature schemes are used.

Our resulting scheme enjoys the constant-size of all parameters together with an efficient computing time. It is therefore the most efficient CLS scheme in the standard model to date. We give in Table 1 the detailed comparison among our CLS scheme and most relevant other existing CLS schemes secure in the standard model.

Table 1. *Comparison between our scheme and some previous CLS schemes in the standard model.* n_u, n_m *are the fixed length corresponding to the parameters of the Water's function. E, P and* M_G *denote the exponentiation in a group G, the pairing computation and the multiplication in a group G, respectively.* $|Sig|, |pk|, Sign, Verify$ *denote the signature size, public key size, signing time, verifying time of a SS secure in the standard model, respectively*

	Sig size	**Public key size**	**Singing time**	**Verifying time**
[10]	$3\|G\|$	$(n_u + n_m + 5)\|G\|$	$5E + \left(\frac{n_u + n_m}{2} + 3\right)M_G$	$6P + \frac{n_u + n_m}{2} M_G + 2M_{G_T}$
[19]	$4\|G\|$	$(n_u + n_m + 4)\|G\|$	$9E + \left(\frac{n_u + n_m}{2} + 7\right)M_G$	$6P + \frac{n_u + n_m}{2} M_G + 2M_{G_T}$
[17]	$3\|G\|$	$(n_u + n_m + 5)\|G\|$	$5E + \left(\frac{n_u + n_m}{2} + 3\right)M_G$	$3P + \frac{n_u + n_m}{2} M_G + 1E + 2M_{G_T}$
[18]	$4\|G\|$	$(n_u + 7)\|G\|$	$6E + \left(\frac{n_u}{2} + 4\right)M_G$	$5P + \frac{n_u + 1}{2} M_G + 1E + 2M_{G_T}$
[7]	$3\|Sig\| + 1\|pk\|$	$1\|pk\|$	$2Sign$	$3Verify$
Ours	$4\|G\|$	$7\|G\|$	$6E + 2M_G$	$3P + 6M_G + 2E$

Paper organization. The next section introduces definition for a CLS scheme. Section 3 gives some tools that we will need for our main construction. In Sections 4 we give our CLS scheme and its security analysis.

2. Certificateless signature scheme

We recall in this section the definition for a CLS scheme, based on the work given in [8]. A certificateless signature scheme requires three actors: a designated authority acting as a Private Key Generator PKG, a signer and a verifier.

Informally speaking, the main difference between a standard signature scheme and a certificateless signature scheme is the way keys are generated. In a CLS scheme, the key generation process is divided into four steps which finally permits to compute the user private key SK_{ID}, computed from both a secret value x_{ID} chosen by the user him/herself and a partial private key D_{ID} generate by the PKG from a master key and the user's identity.

More formally, a CLS scheme consists of seven probabilistic algorithms.

Setup: This algorithm takes as input a security parameter λ and returns the system parameters param and a master secret key *msk*.

Partial-Private-Key-Extract: This algorithm takes as input param, the master key *msk* and a user's identity ID. It returns a partial private key D_{ID} devoted to the user with identity ID.

Set-Secret-Value: This algorithm takes as input the security parameter λ and a user's identity ID and returns the user's secret value x_{ID}

Set-Public-Key: This algorithm takes as input a user's secret value x_{ID}. It returns the user's public key PK_{ID}.

Set-Private-Key: This algorithm takes a user's partial private key D_{ID} and public key PK_{ID}, and his secret value x_{ID} as input. It returns the user's full private key SK_{ID}.

Sign: This algorithm takes param, a message *m*, and a user's full private key SK_{ID} as input. It returns a signature σ .

Verify: This algorithm takes param, a message *m*, a user's identity ID, a public key PK_{ID}, and a signature σ as input. It returns 1 if σ is a valid signature of the message *m* and 0 otherwise.

Regarding efficiency, the main purpose of a certificateless signature scheme is to give a verification phase for which the time complexity does not correspond to the verification of the signature (output by Sign) plus the verification that the partial private key is a correct one (that is, output by Partial-Private-Key-Extract and derived by the PKG).

3. Preliminaries

In this section, we give some useful tools we will need all along the paper. If needed, some other details will be given directly in the description of our scheme, when necessary.

In the sequel, a standard signature scheme SS is given by the three algorithms (KeyGen, Sign, Verify).

3.1. Bilinear groups

Let $G, \widetilde{G}$ and G_T denote three finite multiplicative abelian groups of large prime order $p > 2^{\lambda}$ where λ is the security parameter. Let *g* be a generator of G and $\widetilde{g}$ be a generator of $\widetilde{G}$. We assume that there exists an admissible asymmetric bilinear map $e: G \times \widetilde{G} \to G_T$, meaning that for all $a, b \in Z_p$.

1. $e\left(g^a, \widetilde{g}^b\right) = e\left(g, \widetilde{g}\right)^{ab}$;
2. For $g \neq 1_G$ and $\widetilde{g} \neq 1_{\widetilde{G}}, e\left(g, \widetilde{g}\right) \neq 1_{G_T}$
3. $e\left(g, \widetilde{g}\right)$ is efficiently computable.

In the sequel, the set $\left(p, G, \widetilde{G}, G_T, g, \widetilde{g}, e\right)$ is called a bilinear map group system. In this paper, we consider in the sequel type 3 pairings where there is no efficiently computable homomorphism $\left(\phi: G \to \widetilde{G}\right)$ exist between G and $\widetilde{G}$ in either direction [5].

3.2. Boneh-Boyen signature scheme

Boneh and Boyen have proposed in [2] short signature schemes (named BB for short), secure in the standard model, under the q-SDH assumption [2]. In this paper, we make use of the weak version of the BB signature.

In a nutshell, the BB scheme requires a bilinear map group system $\left(p, G, \widetilde{G}, G_T, g, \widetilde{g}, e\right)$ and works as follows (details can be found in [2]).

KeyGen: The secret key $s \in Z_p^*$, the corresponding public key is $\widetilde{w} = \widetilde{g}^s$.

Sign: On input the secret s, the signature of a message $m \in Z_p$ is obtained by computing $\sigma = g^{1/(s+m)}$.

Verify: On input a message m and the corresponding signature σ, together with the public key w, anybody can verify the validity of $\widetilde{\sigma}$ by checking that:

$$e\left(\sigma, \widetilde{w}\widetilde{g}^m\right) = e\left(g, \widetilde{g}\right)$$

3.3. Pointcheval-Sanders signature scheme

Recently, Pointcheval and Sanders have proposed in [12] a new construction for a signature scheme (called PS in the sequel) with additional features. They prove the security of their construction in the standard model, under a new assumption they have introduced, called PS assumption 1, and given below.

In a nutshell, the PS scheme necessitates a bilinear map group system $\left(p, G, \widetilde{G}, G_T, g, \widetilde{g}, e\right)$ and works as follows (details can be found in [12]).

KeyGen: The secret key is a tuple $(x, y) \in Z_p^*$, and the public key is composed of a random generator $\widetilde{h} \in \widetilde{G}$ and the corresponding tuple $\left(\widetilde{X}, \widetilde{Y}\right)$ where $\widetilde{X} = \widetilde{h}^x$ and $\widetilde{Y} = \widetilde{h}^y$

Sign: On input the secret (x, y), the signature of a message $m \in Z_p$ is obtained by selecting a random $h \overset{\$}{\leftarrow} G$ and outputs $\sigma = (\sigma_1, \sigma_2)$ where $\sigma_1 = h$ and $\sigma_2 = h^{(x+ym)}$

Verify: On input a message m and the corresponding signature $\sigma = (\sigma_1, \sigma_2)$, together with the public key $\left(\widetilde{h}, \widetilde{X}, \widetilde{Y}\right)$, anybody can verify the validity of σ by checking that:

$\sigma_1 \neq 1_{G_1}$;

$e\left(\sigma_1, \widetilde{X}\widetilde{Y}^m\right) = e(\sigma_2, \widetilde{g})$

4. Construction and security analysis

We are now ready to describe our construction. We first describe a high-level intuition of the construction and the security analysis.

4.1. Intuition and security analysis

Intuitively, the master secret key s is a BB signing key and our certificateless signature corresponds to a PS signature by the user, with a BB signature as a generator, that is $h = g^{\frac{1}{s+ID}}$.

The user's partial private key is then a triplet corresponding to a true PS public key, using the above h and a secret key (x, y) which is common to all users. The differentiation between users is done by using a secret value b_i to randomize the PS secret key, as $(x + b_i, y)$. Such key finally helps the user (using x and y "in blind", i.e., without knowing them) to compute the certificateless signature as a PS signature. More precisely, we use the randomization technique of a PS signature, as described in [12].

Regarding security, the unforgeability of the Boneh-Boyen's signature scheme ensures that the adversary cannot derive the partial private key of the target user. The security of the Pointcheval-Sanders' signature scheme then prevents the adversary from forging a valid signature of the target user, on a new message.

Regarding efficiency, the main point is that, using BB and PS signature schemes in the above somewhat generic description, we have found that they are totally compatible in our certificateless setting. In fact, we can arrange the verification equations to have only one single pairing equation to be directly convinced that both the user's whole public key and the given signature are valid.

We now give the details of our construction.

4.2. Detailed description

The construction of our CLS scheme is detailed as follows.

Setup $\left(1^{\lambda}\right)$: The algorithm takes as input the security parameter λ, generates a bilinear map group system $\left(p, G, \widetilde{G}, G_T, g, \widetilde{g}, e\right)$. Let $s, x, y \xleftarrow{\$} Z_p^*$

The public parameters *param* are then

$$param = \left(g, \widetilde{g}, \widetilde{S} = \widetilde{g}^{s}, \widetilde{X} = \widetilde{g}^{x}, \widetilde{Y} = \widetilde{g}^{y}, X = g^{x}, Y = g^{y}\right)$$

and the master secret key is *msk* = s.

Partial-Private-Key-Extract: It takes as input param, *msk* = *s*, and the identity ID of user *i*. For notational simplicity, we suppose that identity $\mathrm{ID}_i \in Z_p^*$. It returns a partial private key

$$D_{ID_i} = \left(D_{1,i}, D_{2,i}, D_{3,i}\right) = \left(g^{\frac{x}{s+ID_i}}, g^{\frac{y}{s+ID_i}}, g^{\frac{1}{s+ID_i}}\right)$$

for user *i*.

Set-Secret-Value: It takes as input user's identity ID_i. It chooses random values $b_i \xleftarrow{\$} Z_p^*$ and returns $x_{ID_i} = b_i$ as user *i*'s secret value.

Set-Public-Key: It takes as input param, x_{ID_2} and returns $PK_{ID_2} = \widetilde{g}^{b_i}$ as the public key for user *i*.

Set-Private-Key: It takes as input x_{ID_i}, D_{ID_i} and returns $SK_i = \left(x_{ID_i}, D_{ID_i}\right)$ as the full private key for user *i*.

Sign: It takes as input param, ID_i, SK_i, and a message *m*. For notational simplicity, we suppose that $m \in Z_p$. The algorithm chooses $r \xleftarrow{\$} Z_p^*$ and computes:

$$U = \left(D_{1,i}\right)^{r} \left(D_{2,i}\right)^{mr} \left(D_{3,i}\right)^{b_i r} = g^{\frac{(x+b_i+my)r}{s+ID_i}}, \; V = \left(D_{3,i}\right)^{r} = g^{\frac{r}{s+ID_i}}$$

$$W = g^{r}, L = \widetilde{Y}^{\frac{b_i}{r}} = \widetilde{g}^{\frac{b_i y}{r}}$$

It returns $\sigma = \left(U, V, W, L\right)$ as the signature on the message *m*.

Verify: It takes as input param, PK_{ID_i}, ID_i, $\sigma = \left(U, V, W, L\right)$ and a message *m*, and computes $U' = \widetilde{S}.\widetilde{g}^{ID_i}$ and $W' = \widetilde{X}.PK_{ID_i}.\widetilde{Y}^{m}.\widetilde{g}$.

It then checks if $e\left(U.V, U'\right).e\left(W, L\right) = e\left(W, W'\right).e\left(Y, PK_{ID_i}\right)$ holds. If this is the case, it outputs 1. Otherwise, it outputs 0.

Completeness. We can easily show that:

$$e(U.V,U').e(W,L) = e\left(g^{\frac{(x+b_i+m.y).r}{s+ID_i}}.g^{\frac{r}{s+ID_i}}, \widetilde{g}^{s}.g^{ID_i}\right).e\left(g^{r}.\widetilde{g}^{\frac{b_i.y}{r}}\right)$$

$$= e\left(g^{r}, \widetilde{g}^{x+b_i+m.y+1}\right)e\left(g^{y}, \widetilde{g}^{b_i}\right) = e(W,W').e\left(Y, PK_{ID_i}\right)$$

4.3. Efficiency considerations

Regarding efficiency, as shown in Table 1, it is obvious that the signature generation necessitates one multi exponentiation in G, two additional modular exponentiations in G and one modular exponentiation in $\widetilde{G}$.

The verification phase consists in executing 2 exponentiations and 4 multiplications in $\widetilde{G}$ and then check the pairing equation. As this the latter can be written

$$e(U.V,U').e(W,L/W') = e\left(Y, PK_{ID_i}\right)$$

it suffices to compute 3 pairings, one multiplication in G, and one in $\widetilde{G}$ for this step.

5. Conclusions

In this paper, we focus on CLS scheme in the standard model, we in fact introduce a new and direct approach to construct an efficient CLS scheme in the standard model, while the existing approaches either make use of the Waters' technique or use the generic conversion technique which both lead to inefficient CLS schemes.

References

[1] S. Al-Riyami and K. G. Paterson (2003), *Certificateless public key cryptography*. In C.-S. Laih, editor, Advances in Cryptology - *ASIACRYPT*.

[2] D. Boneh and X. Boyen (2008), *Short signatures without random oracles and the SDH assumption in bilinear groups*, J. Cryptology, 21(2):149-177.

[3] S. Chatterjee and P. Sarkar (2005), *Trading time for space: Towards an efficient IBE scheme with short(er) public parameters in the standard model*, ICISC'05 Proceedings of the 8th international conference on Information Security and Cryptology.

[4] K. Y. Choi, J. H. Park, J. Y. Hwang, and D. H. Lee (2007), *Efficient certificateless signature schemes*, 5th International Conference on Applied Cryptography and Network Security, ACNS 2007 - Zhuhai, China.

[5] S. D. Galbraith, K. G. Paterson, and N. P. Smart (2008), *Pairings for cryptographers*, Discrete Applied Mathematics, 156(16):3113-3121.

[6] S. Goldwasser, S. Micali, and R. L. Rivest (1988), *A digital signature scheme secure against adaptive chosen-message attacks*, SIAM Journal on Computing.

[7] B. C. Hu, D. S. Wong, Z. Zhang, and X. Deng (2006), *Key replacement attack against a generic construction of certificateless signature*, Conference: Information Security and Privacy, 11th Australasian Conference, ACISP 2006, Melbourne, Australia, July 3-5, 2006, Proceedings.

[8] X. Huang, Y. Mu, W. Susilo, D. S. Wong, and W. Wu (2012), *Certificateless signatures: New schemes and security models*, The Computer Journal.

[9] X. Huang,W. Susilo, Y. Mu, and F. Zhang (2005), *On the security of certificateless signature schemes from Asiacrypt 2003*, in: CANS 05, LNCS 3810, pp.13-25.

[10] J. Liu, M. Au, and W. Susilo (2007), *Self-generated-certificate public key cryptography and certificateless signature/encryption scheme in the standardmodel*, ASIACCS '07 Proceedings of the 2nd ACM symposium on Information, computer and communications security, pp. 273-283.

[11] D. Naccache (2005), *Secure and practical identity-based encryption,* Cryptology ePrint Archive, Report 2005/369.

[12] D. Pointcheval and O. Sanders (2016), *Short randomizable signatures*, In Topics in Cryptology - CT-RSA 2016 -The Cryptographers' Track at the RSA Conference.

[13] A. Shamir, *Identity-based cryptosystems and signature schemes*, In G. R. Blakley and D. Chaum, editors, Advances in Cryptology - CRYPTO'84, pp.47-53.

[14] R. Tso, X. Yi, and X. Huang (2008), *Efficient and short certificateless signature*, In M. K. Franklin, L. C. K. Hui, and D. S. Wong, editors, CANS 08, pp.64-79.

[15] B. R. Waters (2005), *Efficient identity-based encryption without random oracles*, In R. Cramer, editor, Advances in Cryptology - EUROCRYPT 2005.

[16] Q. Xia, C. Xu, and Y. Yu (2010), *Key replacement attack on two certificateless signature schemes without random oracles*, Key Eng. Mater.

[17] H. Xiong, Z. Qin, and F. Li (2008), *An improved certificateless signature scheme secure in the standard model*, Fundamenta Informaticae, vol.88, pp.193-206.

[18] Y. Yu, Y. Mu, G. Wang, Q. Xia, and B. Yang (2012), *Improved certificateless signature scheme provably secure in the standard model*, IET Inf. Secur, vol.6, issue 2, June 2012.

[19] Y. Yuan, D. Li, L. Tian, and H. Zhu (2009), *Certificateless signature scheme without random oracles*. Proc. ISA, LNCS 5576, pp.31-40.

[20] D. H. Yum and P. J. Lee (2004), *Generic construction of certificateless signature*. In H. Wang, J. Pieprzyk, and V. Varadharajan, editors, ACISP 04, pp.200-211.

[21] Z. Zhang, D. S. Wong, J. Xu, and D. Feng (2006), *Certificateless public-key signature: Security model and ecffient construction*.ACNS 06, pp.293-308.